원자력 발전소 안전 필수 시스템의 FMEA분석 결과의 적정성 평가를 위한 템플릿

정세진[O1] 유준범[1] 이장수[2]
[1]건국대학교 컴퓨터-정보통신 공학부, [2]한국 원자력 연구원
{jsjj0728, jbyoo}@konkuk.ac.kr, jslee@kaeri.or.kr

FMEA results evaluation templates for safety-critical systems of nuclear power plants

Sejin Jung[O1] Junbeom Yoo[1] Jang-Soo Lee[2]
[1]Division of computer science and engineering, Konkuk university
[2]Korea Atomic Energy Research Institute

요 약

원자력 발전소의 계측제어 시스템, 소프트웨어와 같은 안전 시스템의 안전성, 신뢰성 등을 확보하기 위해 다양한 위해도 분석 기법들이 사용되고 있다. 이 중, FMEA (failure mode and effects analysis) 현재 가장 많이 사용되는 위해도 분석 기법중의 하나 이다. 하지만 이러한 위해도 분석의 결과에 대한 타당성, 적합성 등의 평가기준 마련은 부족한 상황이다. 이에 본 논문에서는 원자력 발전소의 safety system을 대상으로 하여 FMEA 기법을 이용한 위해도 분석의 가이드 및 평가기준으로 참고할 수 있는 template을 제안한다. 이를 통해 FMEA 분석의 결과를 체계적으로 확인 할 수 있을 것으로 기대한다.

1. 서 론

원자력발전소의 디지털 계측제어 시스템 (Instrumentation and controller)은 높은 수준의 안전성과 신뢰성이 요구되는 안전필수 시스템으로, 실제 사용되기 전에 규제 기관들을 통해 안전성 등이 인증되어야 한다. 위해도 분석 (hazard analysis)은 이러한 시스템의 잠재된 위해도를 분석 하는 작업으로써, 시스템의 잠재된 위해도를 미리 파악해 경감시키거나 줄이도록 할 수 있다. 현재 FMEA (고장모드 및 영향분석)나 FTA (fault tree analysis), STPA (system theoretic process analysis) 와 같은 다양한 위해도 분석 기법들이 적용되고 있다 [1].

FMEA 는 특히 전통적으로 원자력 발전소, 항공, 자동차와 같은 여러 안전 필수 시스템에서 자주 사용되어온 기법으로 시스템, 소프트웨어 컴포넌트의 고장 모드로부터 그 영향을 분석하는 기법이다. FMEA 분석의 중요한 점은 대상 시스템의 컴포넌트 분석 및 고장모드 확인이라고 할 수 있다. 하지만 현재 각종 표준 및 규제 지침에서는 이러한 위해도 분석 기법을 사용한 결과 제시를 통해 안전성 확인의 규제만을 가지고 있을 뿐 위해도 분석 결과의 적정성 평가 등에 대한 방법 및 수준에 대한 내용은 부족하다.

본 논문에서는 원자력 발전소 디지털 시스템 및 소프트웨어의 FEMA 분석에 평가 기준으로 참고할 수 있는 템플릿을 제안한다. 이를 위해 FMEA 기법의 시작점 분석을 수행 하였고, 본 논문에서 제안하고자 하는 템플릿의 커버 범위 또한 확인해 보았다.

2. 고장모드 및 영향 분석 (FMEA)

FMEA는 sub-system, 컴포넌트, function의 잠재적인 고장 모드가 시스템에 미치는 영향을 상위 수준으로 분석하는 귀납적 분석 방법이다. 하위의 작은 모듈/컴포넌트의 문제가 전체 구조에 미치는 영향에 대해 분석하는데 적합한 기법으로, system의 영향 분석을 통해 잠재적인 위험 요소 (hazard)를 분석하는데 효과적이다.

FMEA 분석은 주로 worksheet 형태의 table 을 작성하는 방식으로 진행하며, table은 item, failure mode, causal factor, immediate effect, system effect, hazard, risk, recommendation 등으로 구성 된다. FMEA는 분석의 접근 형태에 따라 functional, structural, hybrid로 구분할 수 있다. FMEA는 고장모드로부터 발생할 수 있는 잠재적인 hazard를 체계적으로 분석할 수 있고, worksheet table 작성을 통해 비교적 쉽게 접근할 수 있다는 장점이 있다.

3. 고장모드 및 영향 분석 템플릿

본 논문에서 제안하고자 하는 고장모드 및 영향 분석(FMEA) 템플릿은 FMEA를 이용한 위해도 분석 시 결과물이 필수적으로 포함해야 하는 요소들을 도출하여 평가에 참고할 수 있도록 한다. FMEA 분석을 위한 템플릿은 시스템 분석 시 안전기능요구사항 에 대한 criteria를 만족하는지 확인할 수 있는 내용으로 구성된 시작점 분석과 이를 기반으로 하여 시스템에 보다 가까운 자세한 형태를 지니는 템플릿 개발 순으로 진행한다.

3.1 FMEA 분석의 템플릿을 위한 시작점 분석

위해도 분석 결과의 적정성 확인/평가는 분석 결과가 '*일정 수준 이상의 분석 결과를 포함하고 있음을 확인*' 이라고 정의할 수 있으며, 이는 '올바른 내용'을 가지고 분석을 시작했는가를 확인하는 시작점이라고 할 수 있다.

FMEA는 컴포넌트의 고장모드로부터 잠재적인 영향을 분석하기 때문에 한 원인 (cause)로부터 그 결과 (result)를 분석하는 기법이라고 할 수 있다. 따라서 FMEA의 시작점은 올바른 '고장 모드'의 확인이라고 할 수 있다.

본 논문에서 대상으로 하는 원자력 발전소의 계통, 계측제어 시스템의 경우 IEEE 603, 379 표준을 통해 시스템 개발 시 지켜야 할 standard, failure criteria를 확인 할 수 있다. <Table 1>은 IEEE 379의 failure criteria [2] 에 대한 표로써 FMEA 분석 템플릿의 시작점에 이용 될 수 있다. 본 논문에서는 <Table 1>의 analysis portion 중 FMEA 분석의 고장모드와 연계될 수 있는 1, 2, 6 번의 항목을 중점으로 한다.

Table 1. IEEE 379의 criteria 분석

IEEE 379의 analysis portion	설명	특징
1. Interconnections between redundant channels	채널 간의 연결 부	System logic 의 갈래
2. system logic	System 기능	
3. Actuation device		System logic에 포함
4. Electrical power supplies	전원 부 분석	
5. Auxiliary supporting features	보조 시스템	
6. Sensing lines	Input 요소	

이러한 시작점에 대해 U.S.NRC (nuclear research commission) 에서는 "Identification of Failure Modes in Digital Safety Systems – Expert Clinic Findings Part2 (RIL 1002)"를 통해 digital I&C safety system의 failure mode에 대해 연구한 바 있다 [3].

RIL 1002[3]에서 제안하고 있는 고장 모드는 system logic과 관련된 failure mode에 초점을 맞추고 있으며 해당 부분들은 주로 'output without demand', 'output value incorrect'와 같이 컴포넌트의 output의 고장모드에 대한 내용들로 구성된다. 하지만 IEEE 379의 failure criteria에 비해 'sensing line'을 커버하지 못하는 등의 부족한 점이 있어 이를 포함해 여러 부분에서 보완의 필요성이 있다.

3.2 FMEA 분석을 위한 템플릿

본 논문에서는 IEEE 379의 failure criteria의 다양한 내용들을 cover하고 기존의 FMEA 분석의 시작점이라 할 수 있는 RIL 1002의 내용을 포함해 원자력 발전소의 디지털 계측제어 시스템 및 소프트웨어의 FMEA 분석 적정성 평가를 위한 확장된 템플릿을 제안한다. 본 논문에서 제안하는 템플릿은 표준의 criteria 에 맞추어 failure mode를 확장하고 기존의 사례들을 종합하여 보완 하였다. 또한 software-intensive 시스템의 특징을 반영하여 보완 하였다.

Table 2. FMEA를 위한 failure mode 템플릿

ID	Failure Mode
1	No output upon demand
2	Output without demand, unwanted response
3	Output value incorrect
4	Output at incorrect time
5	Output duration too short or too long
6	Output intermittent
7	Output flutters
8	Interference
9	Input failure
9-1	No input is inserted
9-2	Input value incorrect
9-3	Input at incorrect time or duration
10	Physical failure of component

<Table 2>는 본 논문에서 제안하는 FMEA 템플릿에 대한 표 이다. 특히 기존 표준의 criteria 중 input failure 에 대한 항목을 기존 사례 및 시스템의 특성에 맞추어 3 종류로 세분화 하여 작성 하였다. <Table 2>를 통해 제안된 고장모드의 템플릿을 통해 FMEA 분석 시 결정하는 컴포넌트, sub-system, function 등의 고장 모드의 적절성 등을 평가하는데 사용 될 수 있다. 템플릿을 이용하여 각 컴포넌트별로 개별적으로 정의되던 고장모드들의 분석 커버 정도를 확인 할 수 있다.

3.3 사례 연구

본 논문에서 제안하는 FMEA 템플릿을 위해도 분석 결과의 적정성 평가에 이용할 때의 커버 정도를 확인하기 위해 기존에 제시된 FMEA 분석 결과와의 비교를 수행 하였다. FMEA는 전통적으로 많이 사용해 오던 기법으로 다양한 분석 결과들이 존재 한다. [4]는 자동 시험 및 연계 프로세서 (ATIP)의 소프트웨어를 대상으로 FMEA를 수행한 논문으로 해당 논문의 failure mode 들은 omission, incorrect realization, function interaction, input, output timing 등이 있다. 이외에도 지난 KNICS 사업에서 연구된 안전성 분석 보고서와 EPRI (Electric power research institute)에서 연구된 보고서 등 다양한 사례들이 존재 한다.

Table 3. [5]와 템플릿의 failure mode 비교 결과 예시

고장 모드	발생 장치 (component)	Template No.
고 신호 유지	아날로그 입력	9
저 신호 유지	아날로그 입력	9
개방 불능	차단기	1
단선, 단락	퓨즈	9-2
시간측정 느림	감시 타이머	5
AD 변환 값 부정확	아날로그 출력	3
프로세서 정지 고장	프로세서 모듈	1, 4

<Table 3>은 [5]에 나타난 FMEA 분석 결과의 고장 모드와 본 논문에서 제안하는 템플릿의 고장 모드와의 관계를 분석한 표의 일부 이다. <Table 3>에 나타난 바와 같이 실제 FMEA 분석은 대상 컴포넌트에 따라 다양한 고장 모드를 적용하고 있으며, 해당 고장 모드들은 본 논문에서 제안하는 템플릿을 통해 표현 가능한 것을 확인 할 수 있다.

Table 4. [6] 과 템플릿의 failure mode 비교 결과 예시

발생 장치 (component)	고장 모드	Template No.
24 VDC Power	Voltage below spec.	3
	Voltage above spec.	3
Governor	Output fails offscale high	3
	Output fails as-is	3
	Output fails offscale low	3
Steam admission valve switch	Fail open	2
	Fail close	1
Governor program interface	Inadvertent logic change	8

[6] 은 EPRI에서 제안한 원자력 발전소 시스템의 위해도 분석 보고서로써 시스템을 다양한 기법을 이용하여 분석한 결과를 제시하고 있다. <Table 4>는 [6]에 나타난 고장모드와의 비교 분석 결과로, 특히 시스템 전체에 특화 되어 있어 본 논문의 템플릿으로 커버가 될 수 있음을 확인 할 수 있다.

이처럼 몇몇 사례 들을 통해 본 논문에서 제안하고자 하는 FMEA 위해도 분석 기법의 적정성 평가를 위한 템플릿이 실제 사례들을 모두 포함하고 있고, 이를 통해 분석 결과들이 적정한 고장 모드 (failure mode)를 가지고 시스템 분석을 수행했는지 평가 하는데 사용할 수 있음을 확인 하였다.

4. 결론 및 향후 연구

본 논문에서는 FMEA 분석 결과의 평가를 위한 위해도 분석 템플릿을 제안하고, 템플릿의 적용 가능성에 대해 확인해 보았다. FMEA 템플릿은 표준의 failure criteria와 기존에 제안된 failure mode 리스트들을 확장하여 제안 되었으며, 템플릿을 이용하여 FMEA를 이용한 위해도 분석에 제시되는 고장 모드들을 카테고리화 하여 평가 할 수 있다. 또한 해당 템플릿은 위해도 분석을 위한 가이드라인으로도 활용 될 수 있을 것으로 기대 한다. 향후 FMEA 뿐만 아니라 다양한 여러 기법들에 대해서도 위해도 분석의 평가에 활용될 수 있는 템플릿에 대해 더 연구할 계획이다.

사 사

이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. NRF-2017R1D1A1B03030065) 과 2017년 정부(미래창조과학부)의 출연금으로 지원을 받아 수행된 주요연구사업의 지원으로 연구한 결과 입니다.

Reference

[1] Clifton A. Ericson, “Hazard Analysis Techniques for System Safety”, John Wiley & Sons, 2005

[2] IEEE, “IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems”, IEEE, 2014.

[3] U.S.NRC, “Identification of Failure Modes in Digital Safety Systems - Expert Clinic Findings”, Part2, 2011

[4] Gee-Yong Park, Dong-Hoon Kim, Dong Young Lee, "Software FMEA analysis for safety-related application software", Annals of Nuclear Energy, Vol 70, pp.96-102, 2014

[5] 한국 원자력 연구원, “KNICS-RPS-AR102”, 2008

[6] EPRI, “Hazard analysis methods for digital instrumentation and control systems”, EPRI, 2013.